ABSTRACT OF THE DISCLOSURE

An encryption method and apparatus that provides forward secrecy, by updating the key using a one-way function after each encryption. By providing forward secrecy within a cipher, rather than through a key management system, forward secrecy may be added to cryptographic systems and protocols by using the cipher within an existing framework. A random-access key updating method can efficiently generate one or more future keys in any order. Embodiments are applicable to forward secret ciphers that are used to protect protocols with unreliable transport, to ciphers that are used in multicast or other group settings, and to protection of packets using the IPSec protocols.